SAMA
November, 2017

SAMA Rules to Implement the CFT Law Provisions

First: Definitions

1. The following terms and phrases – wherever mentioned in the Law and its Implementing Regulation – shall have the meanings assigned thereto unless the context requires otherwise:

A. Law: Combating Terrorism Financing Law issued by the Royal Decree No. 92 dated 11/2/1439 AH.

B. **Transaction:** Includes any disposition of funds, properties, cash or in kind proceeds including but not limited to depositing, withdrawing, transferring, selling, purchasing, loaning, committing, extending of credit, mortgaging, gifting, financing, or exchanging of funds in any currency, whether in cash or checks, payment orders, sticks, bonds or any other financial instruments; or using safe deposit boxes and any other disposition of funds.

C. **Correspondent Relationship:** It is a relationship between a correspondent institution and a respondent institution through a current or other account or related services, such as cash management, international funds transfers, cheque clearing, foreign exchange services, trade finance, liquidity management, or short-term borrowing. The definition shall also cover correspondent relationships established for securities transactions or funds transfers.

D. **Financial Group:** Is a group that consists of a company or of any other type of legal or natural persons that exercises control and coordinating functions over the rest of the group for application of group supervision, together with branches or subsidiaries that are subject to anti-money laundering policies and procedures at the group level.

E. **Legal Arrangements:** The relationship established by a contract between two parties or more which not result legal person, such as trusts or other similar arrangement.

F. **Customer:** any person who takes any of the following actions**:**

a) Arranging, or undertaking a transaction, business relationship or opening account;
b) A signatory to a transaction, business relationship, or account;
c) Assigning an account, transferring rights or obligations according to a transaction;
d) who is authorized to conduct a transaction, or to control a business relationship or an account; or
e) who attempts to take any of previous actions.

Second: Scope of implementation

2. These rules shall be applied by the following financial institutions:

a. Banks operating in the Kingdom.
B. Money exchange operating in the Kingdom.
C. All companies operating in the insurance sector.
D. finance companies.

DRAFT

- **Third: The Financial Institutions' Obligations According to Combating Terrorism Financing Law Risk Assessment**

3. Financial institution shall identify asses and document their terrorism financing risks in writing, and regularly update its terrorism financing risk assessment and any underlying information, and keep both the report and any underlying information readily available for the supervisory authority. The nature and extent of the risk assessment shall be appropriate to the nature and size of the financial institution.

4. Financial institution when assessing its terrorism financing risks, shall give consideration to the following:

a. Customer risk factors and risk factors relating to the beneficial owner or beneficiary;
b. Risk factors emanating from countries or geographic area in which customer operates or the place of origination or destination of a transaction;
c. Risk arising from the nature of products, services and transactions offered and the delivery channels for products and services.

5. When carrying out a risk assessment, a financial institutions shall take into account the any risks identified on the national level and any variables which may increase or decrease the terrorism financing risk in a specific situation, including:

a. The purpose of an account or relationship;
b. The size of deposits or transactions undertaken by a customer;
c. The frequency of transactions or duration of the relationship.

6. Based on the outcome of the risk assessment, a financial institutions shall develop and implement internal policies, controls and procedures against terrorism financing that set out the appropriate level and type of measures to manage and mitigate the risks that have been identified; to monitor the implementation of those policies, controls and procedures; and to enhance them as necessary.

7. For higher level of risks the financial institution shall apply enhanced mitigation measures; for a lower level of risks a financial institution may apply simplified measures to manage and mitigate the risks. Simplified measures shall not be permitted if there is a suspicion of terrorism financing.

8. A financial institution shall identify and assess the terrorism financing risks that may arise from the development of a new product, business practice or delivery mechanism, or from the use of a new or developing technology for new or pre-existing products. The risk assessment shall be carried out prior to the launch of the new product, business practice or delivery mechanism or prior to the use of the new technology. A financial institution shall take appropriate measures to manage and mitigate the identified risk.

- **Customer Due Diligence**

9. A financial institution shall undertake due diligence measures at the following times:

a. Before establishing a new business relationship or opening a new account;

DRAFT

b. Before carrying out a transaction for a customer with whom the financial institution is not in an established business relationship, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
c. c. Before carrying out a wire transfer as prescribed by Article 68 of the Law Whenever there is a suspicion of terrorism financing, regardless of the amounts involved; or
d. Whenever the financial institution has doubts either about the veracity or adequacy of previously obtained customer information or identification data.

10. Due diligence measures shall be based on risk and, at a minimum, comprise of the following:

a. Identify the customer and verify the customer's identity, using reliable, independent source documents, data or information:
    1. For a customer that is a natural person, the financial institution shall obtain and verify the full legal name, residential or the national address, date and place of birth, and nationality;
    2. For a customer that is a legal person or a legal arrangement, the financial institution shall, at a minimum, obtain and verify the name, legal form and proof of existence, the powers that regulate and bind the legal person or legal arrangement, the names of all directors, senior managers or trustees, and the address of the registered office and, if different, the principal place of business.
    3. Depending on the risk posed by a specific customer, the financial institution shall determine whether any additional information must be collected and verified.
b. Verify that any person purporting to act on behalf of a customer is so authorized, and identify and verify the identity of that person in line with subsection (a);
c. Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owners, using information and data obtained from a reliable source, such that the financial institution is satisfied it knows who the beneficial owner is, as following:
    1. For a customer that is a legal person, a financial institution or designated non-financial business and profession shall identify and take reasonable measures to verify the identity of the natural person who ultimately owns or controls 25% or more of the legal entity's shares.
    2. Where no controlling ownership interest exists as stipulated in the previous para (1), or there is doubt whether the controlling shareholder is not indeed the beneficial owner, the identity of the natural person exercising control of the legal person through other means; or, as a last means, the identity of the natural person who holds the position of senior managing official, and verify it.
    3. For a customer that is a legal arrangement, a financial institution shall identify and take reasonable measures to verify the identity of the endower, beholder, the beneficiaries or classes of beneficiaries, and any other natural person exercising ultimate effective control over the legal arrangement.
d. Understand and obtain additional information on the purpose and intended nature of the business relationship, as appropriate.
e. For the legal persons or legal arrangement, the ownership and control structure of the customer should be understood.

11. A financial institution shall verify the identity of the customer and beneficial owners before or during the course of establishing a business relationship or opening an account; or before carrying out a transaction

DRAFT

for a customer with whom the financial institution or designated non-financial business and profession is not in an established business relationship. Where the terrorism financing risk is low, a financial institution may complete verification of the customer's identity as soon as practicable after the establishment of the business relationship if postponing the verification is essential not to interrupt the normal conduct of business and the financial institution shall apply appropriate measures to manage the terrorism financing risk. The financial institution shall take measures to managing the risk in the circumstances where the customer benefit from the business relationship before the verification is completed.

12. In addition to the measures under Section 10 of this rules, a financial institution shall, in relation to a beneficiary of a saving and protection insurance or other investment related insurance policy, apply the following due diligence measures as soon as the beneficiary is identified or designated:

a. For a beneficiary identified by name, take the name of that person whether it is natural or legal person;
b. For a beneficiary designated by class or characteristics or any other means such as deeds , obtain sufficient information concerning the beneficiary to ensure that the financial institution will be able to identify the beneficiary prior to payout;

In all cases, a financial institution shall verify the identity of the beneficiary prior to a payout under the insurance policy or prior to the exercising of any rights related to the policy.

13. A financial institution, when determining whether enhanced due diligence measures are required in relation to a specific policy referred to in section 12, shall take into account risk factors relating to the beneficiary of the policy and, if the financial institution considers that a beneficiary poses a higher risk, shall in all cases identify and verify the identity of the beneficial owner of the beneficiary at the time of payout.

14. A financial institution shall carry out ongoing due diligence on all business relationships in accordance with the risks posed, verify the transition throughout the business relationship to ensure the consistency with customer's data, activities and risk posed by customer. Also It should be ensured that documents, data and information collected under the due diligence process is kept up-dates and relevant by undertaking reviews of existing records, in particular for higher risk customers.

15. A financial institution shall apply due diligence measures to customers and business relationships that existed at the date of coming into force of the Law and this Implementing Regulations. A financial institution shall apply due diligence measures to existing customers and business relationships based on materiality and risk and conduct ongoing due diligence on such existing customers and business relationships at appropriate times, taking into account whether and when due diligence measures have previously been undertaken, and the adequacy of data obtained.

16. A financial institution that is unable to comply with the due diligence obligations may not open the account, establish the business relationship or carry out the transaction; or in relation to existing customers or business relationships, shall terminate the business relationship; and shall in all cases consider submitting a suspicious transaction report to the General Directorate of Financial Intelligence.

DRAFT

17. Where a financial institution has a suspicion of terrorism financing and it reasonably believes that performing due diligence may tip off the customer, it may opt to not carry out due diligence measures and shall submit a suspicious transaction report to the Directorate of financial intelligence , and stating the reasons as to why due diligence was not applied.
18. The financial institution should determine the extent and depth of application of due diligence measures based on types and levels of risk posed by a client or a specific business relationship. When the risks of terrorism financing is high, the financial institution should apply enhanced due diligence procedures consistent with the risks identified. When terrorism-financing risks are low, the financial institution may take simplified measures of due diligence. If there is a suspicion of financing terrorism, simplified due diligence may not be allowed. The simplified measures must be proportional to low risk.

19. A financial institution may rely on another financial institution to perform identification and verification of the customer; identification and verification of the beneficial owner; and to take the necessary measures to understand the nature and intended purpose of the business relationship.

20. If financial institution place reliance on another party as stated in section 19 of this rules, they shall do the following:

a. immediately obtains all necessary information as required under the law and the rules' provisions. .
b. take measures to satisfy that copies of identification data and other relevant documentation relating to the due diligence measures will be made available , and without delay;
c. ensure that financial institution relied upon is regulated, supervised for and has measures in place for compliance with due diligence and record keeping requirements in line with the requirements stipulated under the Law and this rules.
d. Take into account information available with (AMLPC) , the General Directorate of Financial intelligence ,and SAMA with regard to high-risk countries identified.

The ultimate responsibility of all requirements stipulated in this law and its implementing regulation relay on the requesting financial institution.

21. when a financial institution is being relied upon by another domestic or foreign financial institution, confidentially requirements under Saudi law shall not preclude a financial institution from exchanging information as required for the reliant party to determine whether the relied upon financial institutions applies appropriate standards.

22. A financial institution that relies on a financial institution that is part of the same financial group may consider that the financial institution relied upon meets the requirements under Article 19 and 20 provided the group applies due diligence and record keeping requirements in line with the Combating terrorism financing Law and this rules , the implementation of such policies is supervised at the group level by a competent authority and any higher country risk is adequately mitigated by the group's policies and controls.

23. FIs shall takes proper tools to determine whether the person is or has become assignee with a prominent public function in the Kingdom or a foreign country; or with a senior management position in an international organization is consider as "politically exposed person", it shall comprise the following:

DRAFT

a. Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important party officials
b. Directors, deputy directors, and members of the board or equivalent function, of any international organization.

.

24. A family member of a politically exposed person shall include any individual who is related to a politically exposed person by blood or marriage up to the second degree.

25. A close associate of a politically exposed person shall include any natural person who is known to have joint beneficial ownership of a legal entity or legal arrangement or who is in a close business relationship with the politically exposed person, or who has a beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of a politically exposed person.

26. A financial institution shall in relation to politically exposed persons from a foreign country, obtain senior management approval before establishing or continuing such a business relationship; take reasonable measures to establish the source of wealth and the source of funds of the politically exposed person; and conduct enhanced ongoing monitoring on the business relationship; and the same applied in relation to politically exposed persons from the Kingdom, in case of a higher risk of terrorism financing..

27. A financial institution shall take the reasonable measures to determine whether the beneficiaries or the beneficial owner from the saving and protection policy or any other investment insurance policy, before the payout of the policy prior to the exercising of any rights related to the policy, are PEPs, if so, the FI shall inform the senior management before the payout or prior to the exercising of any rights related to the policy, and conduct enhanced scrutiny on the business relationship, and consider making a suspicious transaction report.

- **Record keeping:**

28. Financial institutions must keep all records obtained through due diligence measures, transaction files, commercial correspondence and copies of personal identification documents, including the results of any analysis, for a period of at least ten years after the end of the relationship or a transaction that has been done with walk-in customer.

- **Controls and Policies:**

29. The policies, procedures and internal controls shall be proportionate to the nature and size of the financial institution business and shall address the following:

a. Due diligence measures as required under this law and its Implementing Regulation, including risk management procedures for utilization of a business relationship prior to completion of the verification process;
b. Transaction reporting procedures;
c. Appropriate anti-money laundering compliance management arrangements, including appointment of an anti-money laundering compliance officer at the senior management level;
d. Adequate screening procedures to ensure high standards when hiring employees;

DRAFT

e. Ongoing employee training programs; and
f. An independent audit function to test the effectiveness and adequacy of internal policies, controls and procedures.

30. A financial group shall implement a group-wide program against terrorism financing, apply the internal policies, controls, procedures to all of its branches and majority-owned subsidiaries and ensure effective implementation thereof by all branches and majority-owned subsidiaries. In addition to the issues set out in subsection 29, a group level policy shall address also the sharing of information between all members of the group; the provision of customer, account and transaction information to group-level compliance, audit or combating terrorism financing functions; and the safeguarding of confidentiality and use of the information exchanged.

31. Where the combating terrorism financing requirements of a foreign country are less strict than those imposed under the Law and this Implementing Regulation, a financial institution or designated non-financial business and profession shall ensure that its branches and majority-owned subsidiaries operating in that foreign country apply measures consistent with the requirements under the Law and this Implementing Regulation. If the foreign country does not permit the proper implementation of such measures, the financial institution or designated non-financial business and profession shall inform the Saudi supervisory authority of this fact and take any additional measures necessary to appropriately manage and mitigate the money laundering risks associated with its operations abroad. The financial institution or designated non-financial business and profession shall comply with any instructions received from the supervisory authority in this regard.

- **Correspondent Banks:**

32. Before entering into a cross-border correspondent relationship, a financial institution shall apply the following risk mitigating measures:

a. gather sufficient information about the respondent institution to understand fully the nature of the respondent's business, and determine from publicly available information the reputation of the institution and the quality of supervision, and whether the respondent institution has been subject to a money laundering investigation or regulatory action;
b. assess the respondent institution's anti-money laundering controls;
c. obtain approval from senior management before establishing new correspondent relationships; and
d. clearly understand the respective anti-money laundering responsibilities of each institution.
e. Reach satisfactory convention that a respondent financial institution does not allow the use of its account by shell banks.

33. Where a financial institution registered and licensed in the Kingdom enters into a correspondent relationship in order to receive services from a foreign correspondent financial institution, confidentially requirements under Saudi law shall not preclude the financial institution from providing to the foreign institution the information and documents required for the foreign institution to satisfy itself that the conditions under 32 (a) and (b) are met.

DRAFT

34. Article 68 of the Law shall apply to cross-border wire transfers and domestic wire transfers in any currency, including serial payments and cover payments, which are received, or sent or processed by a financial institution in the Kingdom, including credit or debit or prepaid card, mobile phone or other digital or IT prepaid or postpaid device that are used to effect a person-to-person transfer of funds. The scope of the Law does not extend to a transfer that

a. flows from a transaction carried out using a credit or debit or prepaid card, a mobile phone or any other digital or IT prepaid or postpaid device with similar characteristics and exclusively for the purchase of goods or services, provided the credit or debit or prepaid card number accompanies the transfer flowing from the transaction; or
b. constitutes a transfer or settlement between two financial institutions where both the originator and the beneficiary are a financial institution acting on their own behalf.

35. Originator information shall include:

a) The full name of the originator;
b) The originator account number where such an account is used to process the transaction or in the absence of an account number, a unique transaction number that permits traceability of the transaction; and
c) The originator's address, or customer identification, or date and place of birth.

Beneficiary information shall include:

a) The full name of the beneficiary; and
b) The beneficiary account number where such an account is used to process the transaction or in the absence of an account number, a unique transaction number that permits traceability of the transaction.

36. A financial institution that orders a wire transfer shall include required and verified originator information and required beneficiary information with each wire transfer. In case of a suspicion, an STR shall be submitted according to Article 70 of the Law. If a financial institution cannot comply with its obligations under this provision, it shall not order the wire transfer.

37. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to several beneficiaries, the ordering financial institution shall include in the batch file the required and verified originator information; the required beneficiary information that is fully traceable within the beneficiary country; and the originator's account number of unique transaction reference number.

38. For domestic wire transfers, the obligations set out in Article 36 shall apply unless the ordering financial institution is in a position to make all required originator and beneficiary information available to the financial institution ultimately receiving the wire transfer or competent authorities by other means, in which case the ordering financial institution may only include the account number or a unique transaction reference number that permits the transaction to be linked with the relevant originator or beneficiary information. The ordering institution shall make the required and verified originator and required beneficiary information available within three business days upon receiving a request for such information from the financial institution ultimately receiving the wire transfer or a competent authority.

DRAFT

39. A financial institution shall maintain all originator and beneficiary information in accordance with Article 65 of the Law, as well as the provisions stipulated in this rules.

40. For cross-border wire transfers, a financial institution processing an intermediary element of the payment chain shall ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it, and shall keep all wire transfer information including originator and beneficiary information in accordance with Article 65 of the Law, as well as the provisions stipulated in this rules.

41. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution shall keep a record for ten years of all the information received from the ordering or other intermediary financial institution.

42. A financial institution ultimately receiving or processing an intermediary element of a wire transfer shall have in place and apply procedures for:

a) Identifying wire transfers that lack required originator or beneficiary information;
b) Determining, on a risk basis, when to execute, reject, or suspend a wire transfer that lacks required originator or required beneficiary information; and
c) Taking appropriate risk based follow-up action which may include restricting or terminating the business relationship.

43. A financial institution ultimately receiving a cross-border wire transfer shall take reasonable measures to identify cross-border wire transfers that lack required originator or beneficiary information. Such measures may include post-even monitoring or real-time monitoring where feasible. , if the identity has not been previously verified, a financial institution ultimately receiving the transfer shall verify the identity of wire-transfer sender's information and maintain this information in accordance with Article 65 of the Law.

44. Confidentially requirements under Saudi law shall not preclude a financial institution from exchanging information with other domestic or foreign institutions that are processing any part of the transaction as required to comply with the law and with the provisions under this Article.

45. The receiving or sending or intermediary financial institutions of the wire transfer shall comply with all the requirements issued by the Permanente Committee for Combating Terrorism under the powers granted to it under Article (75) of the Law.

- **Ongoing monitoring:**

46. The financial institution shall monitor and audit transactions on an ongoing basis to ensure that they conform to what the financial institution knows about the client and its business activities, customer risk, and the source of funds. Where the risks of financing terrorism are high, the financial institution must emphasize the degree and nature of the monitoring of the business relationship to determine whether the transaction is unusual or suspicious. The financial institution shall keep the

DRAFT

analysis records for a period of ten years from the date of termination of the relationship or after completion of a transaction for a walk-in customer and make it available to SAMA upon request

- **STR Requirements:**

47. Suspicious reporting requirement stipulated under article 70 of the Law shall include the following:

a) A financial institution that suspects or has reasonable grounds to suspect that funds or parts thereof, are proceeds of crime or are related to terrorism financing or that such funds will be used in acts of terrorism financing, including attempts to initiate such a transaction,
b) A financial institution that suspects or has reasonable grounds to suspect that any of the complicated, high-volume, or suspicious transaction that relates to terrorism financing , including the attempt to execute any of these transactions.

48. The financial institution must raise the suspicion in the form of a detailed report containing all related and available data and information available with any related parties. A financial institution that reports a suspicious transaction must respond without delay and fully to any requests for additional information received from Department, including customer information, accounts or transactions associated with the reported transaction.

49. The reporting obligation under Article 70 of the law applies regardless of the amounts involved.

50. A financial institutions, shall implement indicators of suspected acts of terrorism financing. These indicators shall be updated on a continuous basis according to the development and diversity of methods used to carry out such acts, while complying with the publications of SAMA.

51. The reporting shall be provided as per the form adopted by the Directorate, and as minimum shall include the following information:

A. Names, addresses and phone numbers of those carrying out suspicious transactions;
B. A statement of the suspicious transaction, its involved parties, circumstances surrounding its detection and its current status;
C. Specifying the amount of the suspicious transaction and relevant bank or investment accounts; and
D. The reasons and causes of suspicion on the basis of which the employee made such report.

52. The General Directorate of Financial Intelligence shall further specify the manner in which reports under the law are to be made and the information that shall be transmitted as part of the report.

DRAFT